

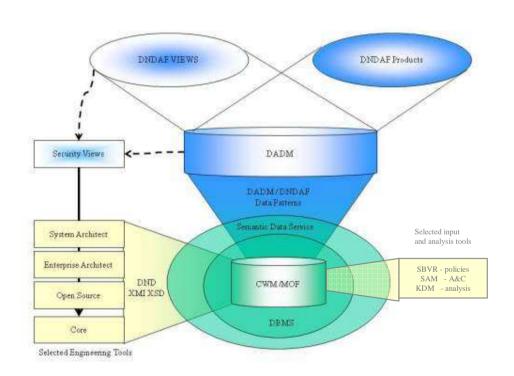
# System Assurance in Support of the C&A Process

Presented by: Leslie Guyatt, Project Director, Enterprise Information Security Environment Project, Department of National Defence, Canada

Software Assurance Forum, 09 March 2010



# Leveraging OMG Standards: SwA Ecosystem+



Common Warehouse Metamodel (CWM)

Knowledge Discovery Metamodel (KDM)

Semantics of Business Vocabulary and Rules (SBVR)

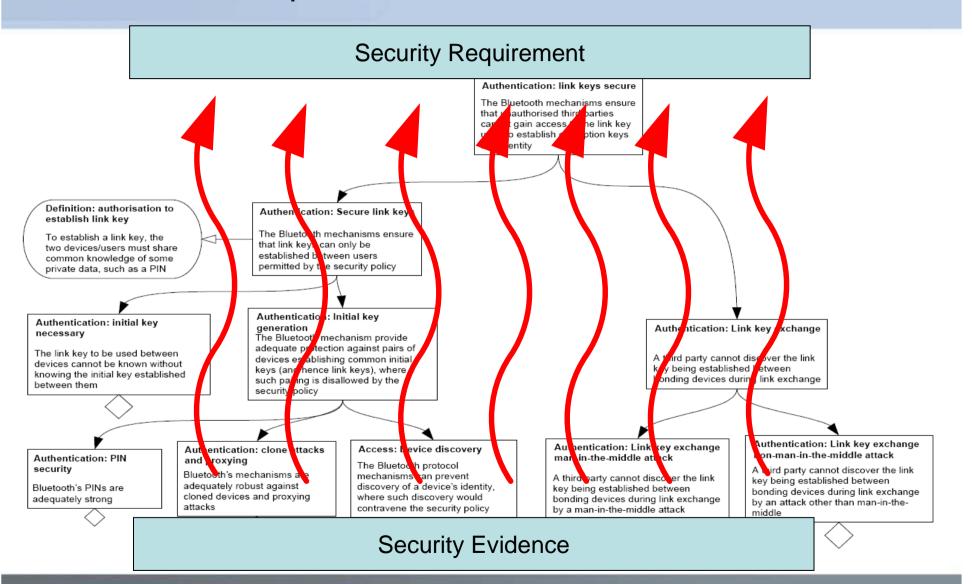
Software Assurance Metamodel (2 standards – WIP)

Unified Profile for DoDAF/MODAF (UPDM)

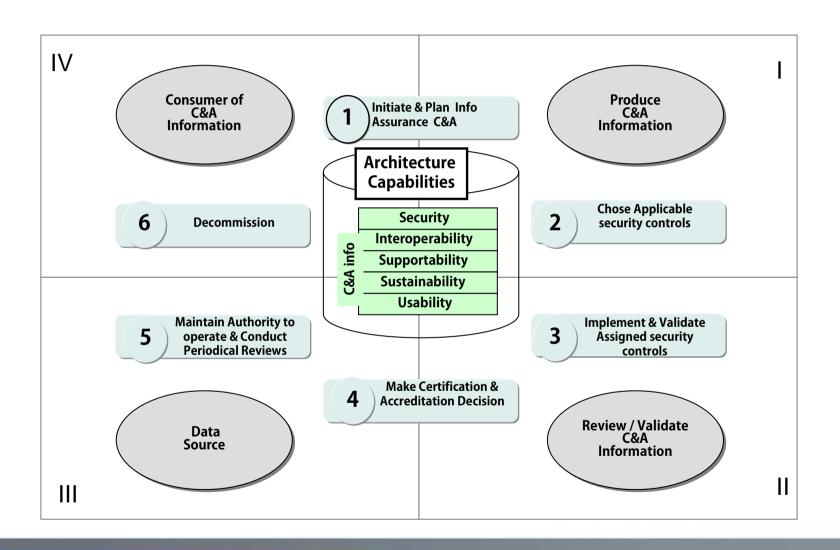
# Information Security Objectives

- Establish standard based, Assurance
   Framework to enable automated, consistent,
   repeatable C&A process
- The Assurance Framework provides common and consistent guidance and communications
  - Capturing a goal-aligned traceability Model
  - Obtaining fact based evidence
  - Assessing residual risk based on discovery noncompliance parts

## A Simple Assurance Case Structure



## C&A Process with the Traceability Model



## Achievable Continuous Assurance

#### System watchdog:

continuous assessment to verify that nothing is sneaking into the development and operational stream

#### Policy enforcement on Data →

- Information discovered in context

IT/IM Mgmt

New/changed Components & Configuration **Automated Analysis** 

- Policy/Rules non-compliance
- Threats and Vulnerabilities
- Changes in policy
- Risk Analysis

Reporting on

Policy/

Rules non-

compliance

Information Value
Chain Feedback Loop
through Customized
Reporting

Rule-based
Policies: Creation
& Administration

## Security Engineering Management

Security Analysis supporting security policies & risk management (Security Engineering and Audit)

### System Architects

Architecture understanding, architecture robustness & rules

## **C&A Management**

Assessment based on established Assurance Case (quality, reliability, security)